ABSTRACT

A digital signature verification protocol utilises a pair of signature components incorporating a pair of private keys, one of which is a long term key and the other of which is a short term key.

The long term key is applied to one of the signature components to reveal the short term key.

The short term key is then used to compute a value of a signature component contained in the signature. If the computed value and received values agree then authenticity is verified.